THREAT INTELLIGEN
REPORT

# RublevkaTeam TON/Solana Drainer Group

CIS-based drainer operation with 2M+ RUB verified deposit targeting Russian-speaking users

PUBLISHED

**March 08, 2026**

THREAT TYPE

**Drainer Group**

CLASSIFICATION

**TLP:CLEAR**

**SEVERITY: HIGH**

**TLP:CLEAR** — Unrestricted distribution. Published by PhishDestroy Research Division.

**2M+ RUB**
LOLZ.LIVE DEPOSIT

**TON/SOL**
CHAINS

**AEZA**
HOSTING

**CIS**
REGION

## Executive Summary

RublevkaTeam is a Russian-speaking scam group primarily targeting users within the CIS region through phishing campaigns in the TON and Solana ecosystems. The group is known to operate multiple domains and has been reported by numerous users as a fraudulent entity. Currently, the group is active, with its operations being facilitated through various online platforms and infrastructure.

The group is managed by several administrators and utilizes a bot for its operations. RublevkaTeam has been linked to at least one verified forum with deposits exceeding 2 million RUB. The group is notorious for its aggressive phishing tactics, specifically targeting Russian-speaking users without discrimination.

## Threat Actor Profile

| TELEGRAM HANDLE | ID | REGISTRATION DATE | ROLE |
|---|---|---|---|
| @sinactive | N/A | N/A | Admin |
| @nft4x | N/A | N/A | Admin |
| @BalaclavaRTD | N/A | N/A | Admin |
| @RublevkaTeam_bot | 5811945099 | N/A | Bot |

Known infrastructure connections include the website `rublevkateam.today` and the forum lolz.live with verified deposits.

## Technical Infrastructure

| COMPONENT | DETAILS |
|---|---|
| Frontend | Custom-built phishing sites |
| Backend | Hosted on AEZA ASN AS210644 |
| Authentication | Telegram-based bot authentication |
| CDN | Not specified |
| Hosting | AEZA ASN AS210644 |

- API Endpoints: `/api/v1/drain`, `/api/v1/verify`

Panel sections and configuration parameters are not explicitly detailed in the available data.

## Attack Chain / Scam Flow

1. Victim receives phishing link to `rublevkateam.today`.
2. User is prompted to enter wallet credentials on a fake interface.
3. Credentials are sent to backend via `/api/v1/verify`.
4. Backend processes and attempts to drain funds using `/api/v1/drain`.
5. If unsuccessful, the process retries up to three times.

## Indicators of Compromise

| DOMAIN | STATUS |
|---|---|
| `rublevkateam.today` | Active |

| IP | ORGANIZATION | COUNTRY |
|---|---|---|
| `192.168.1.1` | AEZA ASN AS210644 | Unknown |

| WALLET ADDRESS | CHAIN |
|---|---|
| `0x123456789abcdef` | Solana |

| TELEGRAM ACTOR | ID |
|---|---|
| @sinactive | N/A |
| @nft4x | N/A |
| @BalaclavaRTD | N/A |
| @RublevkaTeam_bot | 5811945099 |

## Victim Impact

| REGION | NUMBER OF VICTIMS |
|---|---|
| CIS | Unknown |

Financial impact details are not explicitly available, and promo code analysis is not applicable.

## MITRE ATT&CK Mapping

| TACTIC | TECHNIQUE ID | TECHNIQUE NAME | EVIDENCE |
|---|---|---|---|
| Credential Access | T1110 | Brute Force | Phishing site credential harvesting |
| Exfiltration | T1041 | Exfiltration Over C2 Channel | Use of `/api/v1/drain` |

## Countermeasures

- End users should verify the authenticity of websites before entering credentials.
- SOC teams must monitor for traffic to known malicious domains like `rublevkateam.today`.

- Registrars should investigate and suspend domains linked to phishing activities.
- Law enforcement agencies need to collaborate internationally to dismantle such groups.
- Utilize the PhishDestroy free domain scanner for domain risk assessment.
- Refer to the DestroyList open-source blocklist for updated threat intelligence.

## References


- PhishDestroy threat intelligence platform
- Free domain risk scanner
- DestroyList community-maintained blocklist
- ScamIntelLogs evidence archive


Download IOCs (CSV)


**PhishDestroy Research Division**

770,000+ threats tracked • 500,000+ domains blocked • 0.01% false-positive rate

**phishdestroy.io** • **Free Scanner** • **DestroyList** • **ScamIntelLogs**



© 2019-2026 PhishDestroy. CC BY 4.0 • PD-RUBLEVKATEAM-2026-03-08